National Infrastructure Advisory Council (NIAC)

Convergence Working Group

Status Report
July 11, 2006

George H. Conrades
Executive Chairman
Akamai Technologies

Greg Peters
Managing Partner
Collective IQ Partners

Margaret Grayson
President, Grayson and Associates

Overview

- Purpose
- Status of *Next Steps* from Last Meeting
- Timeline
- Actions
- Directional Recommendations
- Next Steps

Purpose

- Mission: The Convergence Study Group will investigate important questions and make recommendations regarding the protection of SCADA and Process Control Systems from cyber threats.

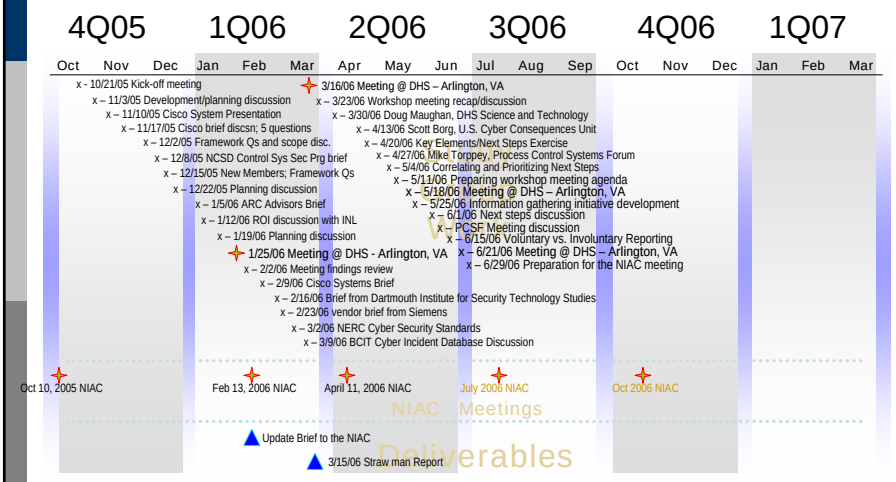
The Five Framework Questions

- ***Security as an Enabler*** **-** How do we position Cyber Security as a contributor and an enabler to achieving reliability, availability and safety goals in the management of SCADA and Process Control Systems?
- ***Market Drivers*** **-** What are the market drivers required to gain industry attention and commitment to research and product development?
- ***Executive Leadership Awareness*** **-** How do we best generate executive leadership awareness to assist in creating a culture and environment that values the protection of SCADA and Process Control Systems from cyber threats?
- ***Federal Government Leadership Priorities*** **-** What are the appropriate Federal Government leadership roles and priorities in identifying threats, vulnerabilities, risks and solutions?
- ***Improving Information Sharing*** **-** What are the obstacles and recommendations for improving information sharing about Process Control Systems and SCADA threats, vulnerabilities, risks and solutions?

Status of *Next Steps* from Last Meeting

- ✓ Address consequences element with Scott Borg, US-CCU
  - Integrated consequences into recommendation for improving Executive Leadership Awareness, informed discussions on Improved Information Sharing
- ✓ Conduct CEO information gathering
  - Attended Process Control Systems Forum Spring Meeting, interviewed eight executive level participants to validate initial findings
- ✓ Further develop potential recommendations
  - Identified 9 draft recommendations to address key elements/framework questions
- ✓ Consult University of Georgia Department of Risk Management
  - Collaborating with Malcolm Baldridge Award board of overseers to communicate SCADA/ PCS cyber security message.

Time Line



Actions

- Held 11 weekly conference call discussions with subject matter experts to address key issues identified during the discovery process
- Held third and fourth face-to-face workshop meetings at DHS
- Used the Five Framework Questions to identify key elements of the desired end states
- Developed process to interrogate the key elements of the framework questions
- Attended the Process Control Systems Forum Spring Meeting to gather executive level perspective on the study's initial findings
- Developed 9 draft recommendations for identified key elements

Directional Recommendations

- Executive Leadership Awareness:
  - Advocate the dissemination of information on threat, vulnerabilities and economic impacts to owner-operators, vendors and government executives in CIP
  - Recommending specific plan in final report based on findings
- Government Leadership:
  - Evaluate recommending a study to investigate the potential role of Sarbanes-Oxley in ensuring the protection of SCADA and PCS from cyber threats
  - Working with Malcolm Baldridge board of overseers to communicate SCADA/PCS cyber security message
  - Recommending that government R&D funding coordinate based on priorities identified by cross-agency CSIA IWG annual reports
  - Recommend funding to accelerate and promote Control Systems Security Program's Vulnerability Assessment Tool to improve owner-operators security posture

Directional Recommendations *(continued)*

- To Improve information sharing:
  - Recommend collection of incident data through protected, trusted mechanism with CERT/CC to provide for more accurate CIP risk assessments
  - Provide CERT/CC program with the necessary resources to rapidly ramp up their SCADA/Process Control Systems training and engineering consulting services needed to build the trusted relationships that will facilitate incident information sharing
  - To get the right information to the right people at the right time, recommend acceptance of and collaboration in efforts to develop the Congressionally-mandated and President-directed Information Sharing Environment.
  - Recommend drafting formal request to intelligence community (RFI) to assess the cyber threat to SCADA and Process Control Systems and communicate that information with Critical Infrastructure owner-operators

Next Steps

- Investigate outstanding key elements
- Investigate the role of the Malcolm Baldridge Quality Award in raising executive awareness and government leadership in security of SCADA and PCS
- Continue executive information gathering to validate draft recommendations
- Finalize recommendations
- Draft the Final Report for October submission to the NIAC

Discussion

- Questions?